



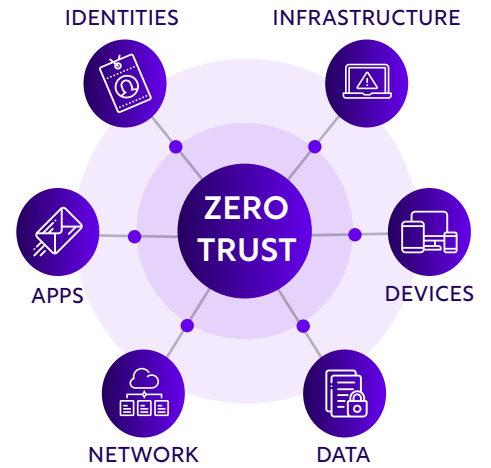
# Cyber Security Services

Advanced cyber security services that help organisations assess, implement and manage a Zero Trust security with Microsoft technologies, underpinned by our **24/7/365 Cyber Security Operations Centre (CSOC)**.

## Background

Cyber security is a top business priority; however, the way that organisations approach security has radically changed. Traditional perimeter-based security methods are no longer effective as cloud services and remote working has redefined the security perimeter. Instead, organisations are embracing Zero Trust Networking to adapt to the complexity of modern working.

Alongside the journey to Zero Trust, organisations are realising the need for continual threat detection and response to reduce cyber threats and their impact. Rather than take on the burden and costs to setup a Cyber Security Operations Centre, companies are partnering with MSSP's to benefit from proactive managed security services and advanced expertise.



## Our managed security services

Our cyber security services leverage Microsoft technologies to help organisations at any stage of their security journey assess, implement and manage an advanced cyber security strategy. We believe in giving practical expertise and support to ensure that our clients maximise the value from their technologies, reduce organisational risk and stay ahead of the rapidly-evolving threat landscape.

### Assess

Threat Check Workshop or Zero Trust Security Assessment

- ✓ Identify active threats and vulnerabilities
- ✓ Outline risks, severity and impact
- ✓ Prioritise recommendations to mitigate risk and improve security posture

### Implement

Security Technology Implementation

- ✓ Define and plan a phased security roadmap
- ✓ Implementation of security technologies to achieve zero trust
- ✓ Advise on an evolving security strategy and approach

### Manage

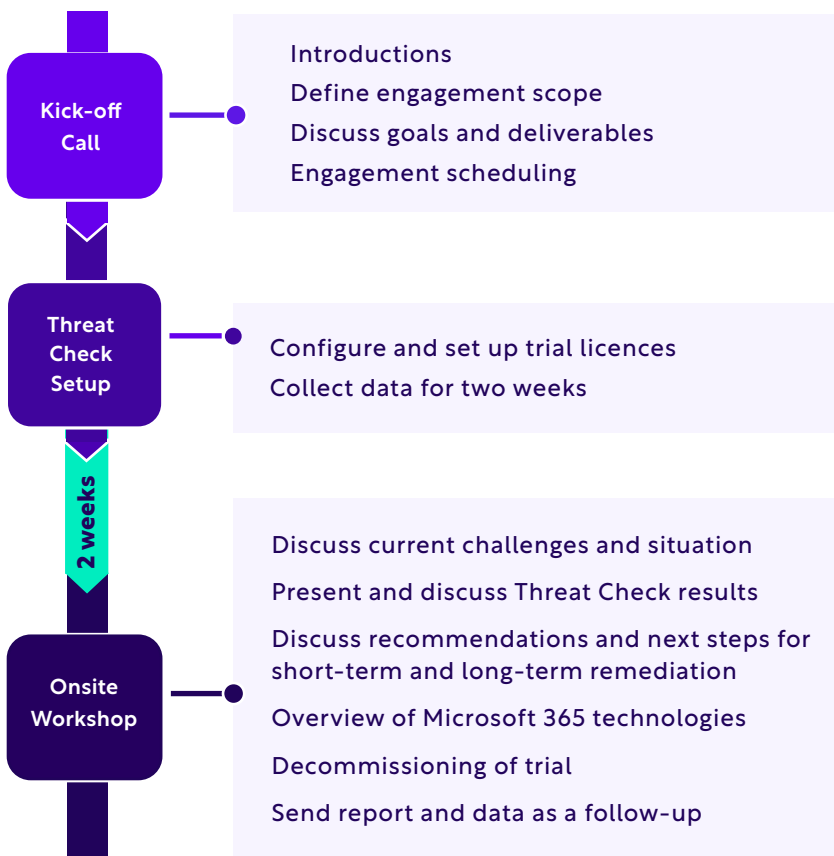
Managed Security Services (MDR & MXDR)

- ✓ 24x7x365 UK-based CSOC with threat detection and investigation
- ✓ Threat remediation and automated response via security playbooks
- ✓ Service reports, recommendations and strategic guidance



Our Microsoft Threat Check Assessment provides a high-level overview of your security posture, and carries out a Threat Check using a Microsoft 365 E5 trial to scan your digital estate to identify active threats and vulnerabilities across email, identity and data. Results are gathered, analysed and presented via a report and on-site workshop to identify key threats and outline prioritised remediation steps.

## Engagement process



## Review your wider security posture

Our Zero Trust cyber security assessment includes the Threat Check as well as a more in-depth review of your wider security situation - please see the next page for more details.

## Engagement overview

The Threat Check uses a **Microsoft 365 E5** trial to scan and monitor your digital estate, detecting and highlighting active and potential threats.

This uses three key technologies within Microsoft 365:

**Entra ID** (formerly Azure Active Directory) – Detects user identity threats, such as compromised credentials and attempted sign-ins.

**Microsoft Defender for Office 365** – Detects threats to email and data, such as malware and phishing attempts.

**Microsoft Defender for Cloud Apps** – Raises alerts on user or file behaviour anomalies in cloud apps leveraging their API connectors.

## Optional inclusions

In addition, the following areas can be added to the Threat Check but would be discussed during the kick-off call as they require additional configuration or may impact end users:

**Microsoft Defender for Identity** – Provides visibility into on-premise alerts and detects vulnerabilities, such as plain text credentials.

**Attack Simulator** – Enables a controlled phishing attack simulator to be carried out to assess end user awareness and risk.

**Shadow IT Discovery** – Generates a cloud app discovery report, which reveals approved and unapproved cloud applications being used to store company data.



Our cyber security assessment reviews your current cyber security posture against a Zero Trust model, reviewing your IT security maturity, identifying risks and vulnerabilities and providing prioritised risk mitigation recommendations to help you adopt an advanced, Zero Trust security model.

Through a combination of consultative reviews and our technical Threat Check assessment, we analyse your security posture, covering six foundational security areas: Identity, Devices, Applications, Infrastructure, Networks and Data.

## Security areas

Area	Description
Identities	Zero Trust begins with strong identity and access management. We assess how identities are managed, secured and authenticated.
Devices	Devices create a massive attack surface area; we will review how your endpoints are managed, monitored and secured – whether company-owned or personal devices (BYOD).
Applications	We focus on discovering shadow IT and reviewing application access, permissions, usage and monitoring – whether on-premise, hybrid or SaaS.
Network	Zero Trust moves away from a network perimeter focus towards intelligent access controls; however, network security must still not be overlooked. We review network controls to evaluate your network security in a Zero Trust model.
Infrastructure	Your infrastructure is a critical attack vector used to exploit vulnerabilities. We assess how your infrastructure is managed and secured, and measures for anomaly detection.
Data	Data should remain secure even if it leaves company apps, networks, infrastructure or devices. We evaluate your data security (such as labelling, encryption and classifications) to review your data protection measures.

## Approach

We use non-intrusive security technology to scan your digital estate over two weeks, picking up active and potential threats and vulnerabilities to identify security weaknesses.

Alongside this, our security consultants will complete a comprehensive audit to review your cyber security.

## Benefits

**Holistic security view** – Our assessment service provides a view of your security posture so that you gain a clear picture across your digital estate.

**Detect live threats** – The security toolset report will highlight any active security threats that could need to be immediately remediated.

**Reduce risk** – We help identify potential security vulnerabilities so that you can quickly mitigate these risks before an issue arises.

**Clear security priorities** – We identify clearly prioritised recommendations to aid security decision making and help you define your security roadmap to implement the most effective remediations first.

**Speak to an expert** – Rather than simply sending a report, one of our security consultants will come to your offices to present the findings and allow time for discussions and questions you may have.



## Assessment scope

Our cyber security assessment includes the following elements but additional components can be added.

### Identity

- ✓ MFA
- ✓ Conditional Access
- ✓ Single-sign on (SSO)
- ✓ Password hygiene
- ✓ Legacy Authentication
- ✓ Identity Security Posture
- ✓ Phishing Attempts
- ✗ DMARC/DKIM/SPF

### Devices

- ✓ Endpoint protection
- ✓ MDM, MAM & BYOD
- ✓ Web filtering
- ✓ Vulnerability management
- ✓ Patch management
- ✓ Endpoint encryption
- ✓ Endpoint detection & response (EDR)
- ✗ Hardware

### Applications

- ✓ Shadow IT discovery
- ✓ Abnormal behaviour monitoring
- ✓ OAuth app consent
- ✗ APIs
- ✗ Custom applications

### Network

- ✓ IDS/IPS
- ✓ Network traffic monitoring
- ✓ SIEM (log analytics)
- ✗ Firewall configuration and management
- ✗ Network segmentation

### Infrastructure

- ✓ Privileged Identity Management (PIM)
- ✓ Just in Time (JIT)
- ✓ Domain controllers
- ✓ Server encryption
- ✓ Infrastructure monitoring
- ✓ Event log monitoring
- ✓ Server patching
- ✓ Email security
- ✗ Server configuration

### Data

- ✓ Data classification
- ✓ Labelling policies
- ✓ Data encryption
- ✓ Data Loss Prevention (DLP) policies
- ✓ Ransomware protection
- ✗ File and folder permissions

## Assessment deliverables

On completion of the audit and scanning, our security consultants will review the findings and present them within your report. This includes:

**Overview:** An overall view of your security posture and security maturity.

**Risks and Threats:** Receive a detailed breakdown of active and potential risks and vulnerabilities found across your digital estate. This will outline the threat, its severity and potential impact.

**Dashboards:** We will share the technical findings via dashboards, charts and reports to give you the detail into any weaknesses and risks.

**Mitigations and Recommendations:** We will outline the recommended mitigations and clearly prioritise the most effective remediations to make to aid your strategy and decision making.

**Onsite or Remote workshop:** Our security consultants will deliver the results and discuss the findings and recommendations with you either onsite or via a remote workshop.





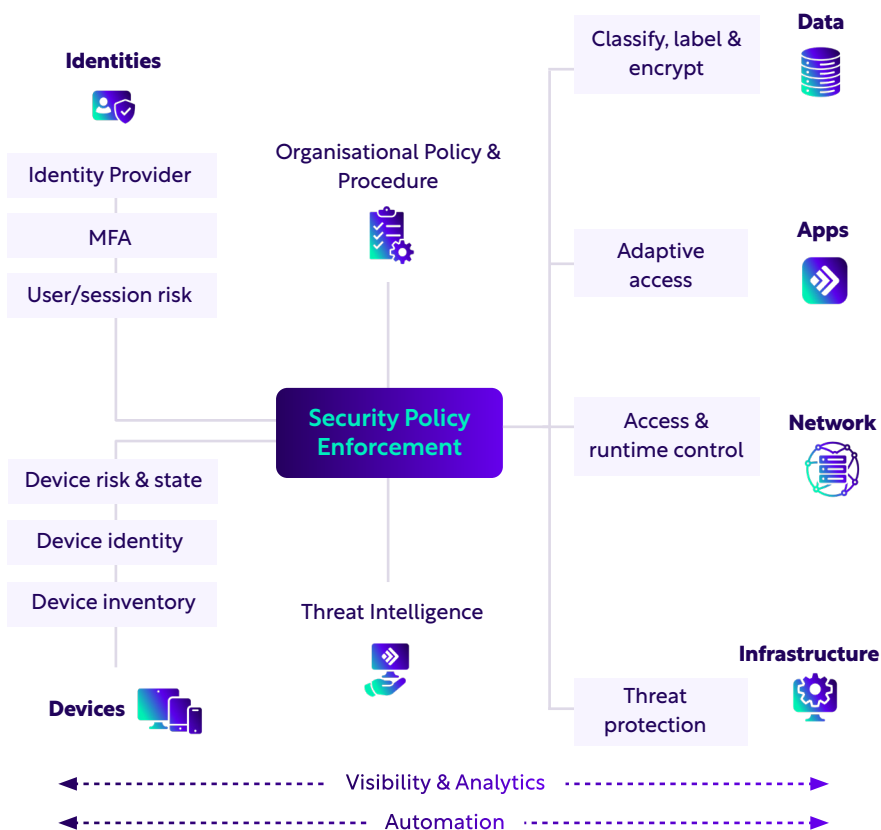
Our security implementation services help you implement a Zero Trust model that is underpinned by leading Microsoft security technologies. Following an assessment of your organisation's situation, risks and goals, we will follow our project methodology with clear communication and milestones to implement the technologies to secure and protect your data, people and organisation.

## Phased security approach

While a Zero Trust model is most effective when implemented and integrated across your entire digital estate, most organisations will need to adopt a phased approach. As Zero Trust is designed for a cloud-first mobile-first environment, organisations may be held back by legacy systems.

For a successful transition, it is worth implementing a Zero Trust model as part of your wider digital transformation – adopting new technologies as legacy systems and existing environments are migrated to the cloud. By phasing the adoption, the transition can focus on prioritising the most effective and least challenging changes for maximum benefit to your security posture, whilst ensuring a smooth transition for your staff.

## Zero trust architecture



## Microsoft 365

Microsoft is a leader in security technology and we recommend implementing Microsoft 365 to achieve Zero Trust.

Microsoft 365 includes a comprehensive and advanced suite of integrated security products, such as Microsoft Cloud App Security, Intune, Azure Information Protection and the Microsoft 365 Defender solutions. Using these products allow organisations to secure and protect their staff, devices and data with a modern Zero Trust approach.

## Why Microsoft 365?

- The biggest strength of Microsoft 365 is the **unparalleled scale** of its underlying platform: the Intelligent Security Graph. This uses machine learning and advanced AI to continually improve and learn from the trillions of signals that Microsoft receive daily.
- Microsoft's products work perfectly together, integrating and feeding data across all solutions. With **one integrated toolset**, you benefit from simplicity and reduced complexity for quicker detection.
- Using Microsoft 365 potentially removes many additional **third party costs**.
- Microsoft 365 not only provides the security tools, but offers **centralised management capabilities** so that changes in security and compliance can be quickly updated and immediately enforced.
- Ensures a **smooth user experience** for your staff so they are protected but productivity is not impacted.

## Security maturity roadmap

Every organisation's cyber security roadmap will be unique, but a 'typical' strategy with common milestones and products could look like:

### Traditional

Traditional perimeter-based security model securing the internal network. Difficulty securing and managing devices and a lack of visibility over cloud services and data once it leaves the network.

**Methods:**

Network perimeter security model  
Firewalls and IDS  
Anti-virus/malware protection  
Single factor authentication

### Modern

Moving towards dynamic security with a focus on data and identity protection (Multi-Factor Authentication, Conditional Access) to gate access and increased analytics into threats.

**Products:**

Entra ID (Azure Active Directory)  
Microsoft Defender for Identity  
Microsoft Defender for Office 365

### Advanced

Mobile devices are secured to enable BYOD and centralise management, cloud threat protection is in place and usage monitored. Analytics are being used to assess user behaviour and identify threats.

**Products:**

Intune - MDM & MAM  
Microsoft Defender for Cloud Apps  
Microsoft Defender for Endpoint  
Web Filtering

### Optimal

Strong use of machine learning and automation with real-time threat detection and response. Data is self-protecting and there is zero trust across the entire network.

**Products:**

Azure Information Protection  
Microsoft Sentinel  
Threat Hunting

## Building the right strategy

All organisations will be at different stages of their security journey and have different priorities and challenges that will shape their strategy. We work closely with our clients to build the right strategy, forming the most appropriate phasing to meet your unique requirements.

The phasing of your roadmap would be determined by:

- Focusing on critical security changes to ensure **key baseline protection**
- Determining complexity of changes against your digital estate so low complexity and highest value changes are delivered first to **deliver value quickly**
- Reviewing any **business priorities** or requirements with timescales (such as compliance certifications)
- Assessing **current technologies** and any legacy infrastructure to determine any potential challenges
- Ensuring the **best use of licensing** by implementing technologies that you may already be paying for first
- Reviewing your **cloud migration strategy** and wider IT roadmap to ensure your security strategy aligns



## Get certified

We can also help you gain cyber security accreditations for compliance, such as:



- Cyber Essentials
- Cyber Essentials Plus
- ISO27001

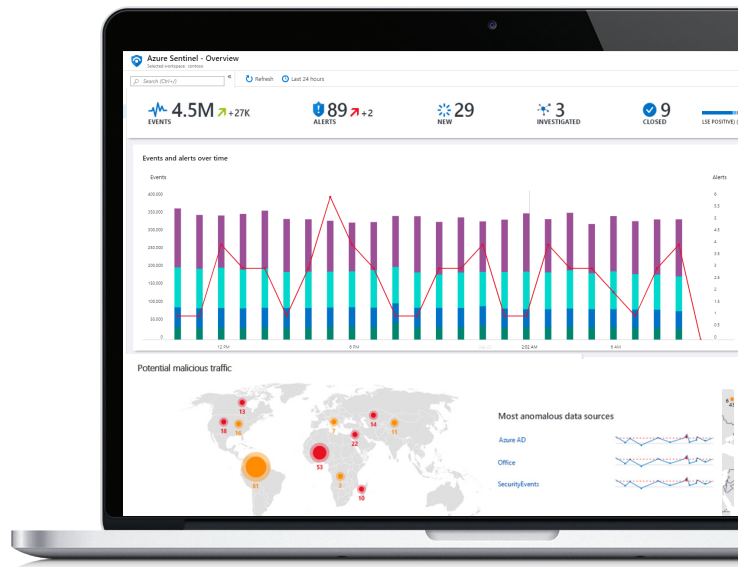


Advanced Managed Detection & Response (MDR) and Managed Extended Detection & Response (MXDR) services, powered by Microsoft 365 Defender and Microsoft Sentinel, delivered via our 24x7x365 UK-based Cyber Security Operations Centre (CSOC).

## Staying ahead of evolving cyber threats

Cyber security attacks are increasing in frequency and sophistication, which is why cyber security is a key business priority. Today, organisations need to reduce the likelihood of an attack, proactively detect threats, and rapidly respond to reduce potential business impact. To achieve this, organisations need the right processes and technology in place with a team of highly skilled security experts, however for many, this is uneconomical to build and maintain internally.

Delivered via our 24x7x365 UK-based CSOC, our Managed Security Services help organisations stay protected in today's rapidly evolving threat landscape. Through our highly qualified SecOps team, mature processes and underpinned by advanced Microsoft security technologies, we believe in bringing affordable enterprise-level security to organisations of any size.



## Our managed security services

Our Managed Security Services leverage Microsoft technologies to help organisations detect, investigate, hunt and respond to cyber security threats. We provide flexible MDR and MXDR services, allowing organisations to choose the right level of protection to meet their security requirements and internal capabilities.

### MDR Endpoints

Advanced threat detection and remediation services to protect all of your endpoints.



### MXDR Advanced

Extended threat detection and response across your cloud services.



### MXDR Premium

End-to-end visibility, remediation and protection across your entire estate (cloud, hybrid & on-premise).



## Benefits of our managed security services

**Modern and innovative CSOC** – We have built our 24/7 CSOC to make best use of technical innovations and cutting-edge cloud security technologies to deliver an advanced managed service. Underpinned by our team of highly skilled and experienced CSOC analysts, our team protect your organisation around-the-clock.

**Leading technical architecture** – Built on Microsoft 365 Defender and Microsoft Sentinel, our CSOC architecture is built to best-practice to benefit from cutting-edge automation, machine learning, AI and integration to reduce alert noise, automate common tasks and accelerate threat detection and response times.

**Proactive and preventative protection** – We take our services a step further by building in pre-emptive protection through advanced threat hunting and cyber threat intelligence to proactively block emerging and unknown threats before they occur.

**Rapid threat detection and response** – Through our skilled SecOps team, advanced technology and use of automation, we ensure cyber threats are quickly identified, investigated and remediated – reducing the likelihood and potential impact of successful attacks, to keep your organisation ahead of evolving threats.

**Mature services** – With over 20 years experience delivering managed services, we have a mature service delivery model to complement our technical skills. Through continual service improvement, service governance and reporting we ensure optimal service delivery.

**Risk reduction** – With proactive threat detection, investigation, hunting and response, your organisation is better protected and cyber risk is greatly reduced. This helps you to reduce cyber insurance premiums, meet compliance regulations and benefit from greater peace of mind against increasingly costly attacks.any size.

## What's included?

24x7x365 CSOC

Flexible coverage  
Endpoints, Cloud or Hybrid

24x7 monitoring

Proactive Cyber Threat  
Intelligence (CTI)

Threat Detection

Threat Triage & Investigation

Rapid Threat Response

Proactive Threat Hunting

Service Governance &  
Reporting

Security Reviews &  
Recommendations

Streamlined Service  
Transition

Phishing Simulation

## Our CSOC Metrics

<5 mins Mean Time to Acknowledge (MTTA)

<15 mins Mean Time to Close (MTC)

50% Incidents closed by automation

## Microsoft security

Our MDR & MXDR services are built on Microsoft 365 Defender and Microsoft Sentinel - Microsoft's integrated XDR and SIEM/SOAR technologies.

By using these advanced cloud technologies, we can rapidly detect sophisticated threats across any data source. Through Sentinel's SOAR capabilities and our security playbooks, common threats are automatically remediated while sophisticated attacks are investigated by our team of highly skilled CSOC analysts to ensure rapid response.

## Microsoft Intelligent Security Association

 Microsoft Security

 Microsoft Verified Managed XDR Solution



hello@chorus.co.uk






01275 398 900



www.chorus.co.uk



## Which level of service is right for you?

SERVICE COMPARISON		 MDR Endpoints	 MXDR Advanced	 MXDR Premium
24x7x365 UK-based CSOC		✓	✓	✓
Analysts available by phone 24x7		✓	✓	✓
30 minute high severity SLA		✓	✓	✓
Containment and response actions		✓	✓	✓
Chorus proprietary analytic rules		✓	✓	✓
Microsoft Security suite coverage	Defender for Endpoint	✓	✓	✓
	Defender for Identity		✓	✓
	Defender for Cloud Apps		✓	✓
	Defender for Office		✓	✓
	Defender for Cloud		✓	✓
	Azure services		✓	✓
Microsoft Sentinel custom integration				✓
Threat Detection & Response Coverage	Endpoints	✓	✓	✓
	Entra ID Identities	✓	✓	✓
	Servers	✓	✓	✓
	Active Directory Identities		✓	✓
	Non-Azure cloud services			✓
	Networking log sources (Firewalls/Switching/APs)			✓
	3rd Party APIs/Logs			✓
Weekly security service reports		✓	✓	✓
Cyber Essentials aligned TVM report		✓	✓	✓
Endpoint threat hunting		✓	✓	✓
Cyber Threat Intelligence		✓	✓	✓
Standard security playbooks		✓	✓	✓
Security recommendations & guidance		✓	✓	✓
Service governance		✓	✓	✓
Extended threat hunting			✓	✓
Custom security playbooks			✓	✓
MITRE ATT&CK framework mapping				✓
External attack surface monitoring				✓

## Why Chorus?

Modern 24/7 UK-based CSOC combining cutting-edge cloud security technologies with highly skilled security experts to deliver rapid threat detection and response

Advanced MDR & XDR services built upon Microsoft's industry-leading XDR & SIEM/SOAR solutions: [Microsoft 365 Defender](#) and [Microsoft Sentinel](#)

Member of [Microsoft Intelligent Security Association \(MISA\)](#) and [Microsoft-verified MXDR](#) solution with Microsoft designations and Advanced Specialisations in Security

[Innovative and preventative approach](#) with a focus on automated threat remediation and proactive threat intelligence to block emerging threats

Accredited to [leading industry quality & security standards](#)

Rapid threat detection and response [CSOC metrics](#) that are far higher than industry benchmarks

[Collaborative partnership](#) to help build the right model to suit your organisation and meet your requirements

Combine [best of both worlds](#) with the maturity of a large provider and personal service and agility of a trusted partner

### Lite MDR & MXDR

**Lite version** of all three services available that only covers alerts classified as Medium or High in Microsoft Sentinel.



Chorus is a transformative Managed Security Service Provider (MSSP), providing a unique alternative to the traditional cyber security provider.

As one of the UK's leading Microsoft partners, we are on a mission to build a more secure world of business, where you can thrive with modern Microsoft technology, in a new era of cyber threats. Through our UK-based 24/7/365 Cyber Security Operations Centre (CSOC), we combine the expertise of some of the best minds in the industry with the innovative use of automation and Microsoft's advanced security stack to achieve this.

We are a leading Microsoft partner and proud to be members of the Microsoft Intelligent Security Association (MISA), making us one of the most reliable and trusted Microsoft-focused security companies across the globe.

Our Managed Security services have been awarded Microsoft-verified MXDR solution status, proving the calibre of our service.

## Microsoft Intelligent Security Association



Cyber-security Information Sharing Partnership



## WHAT NEXT?

If you would like to find out more information about our cyber security services, or have any questions, please get in touch with our team today.



hello@chorus.co.uk



01275 398 900



www.chorus.co.uk